



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/686,410	10/14/2003	Eshwari P. Komarla	42P17160	6852
8791 7590 01/07/2008 BLAKELY SOKOLOFF TAYLOR & ZAFMAN 1279 OAKMEAD PARKWAY SUNNYVALE, CA 94085-4040			EXAMINER REZA, MOHAMMAD W	
			ART UNIT 2136	PAPER NUMBER
			MAIL DATE 01/07/2008	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/686,410	Applicant(s) KOMARLA ET AL.	
	Examiner Mohammad W. Reza	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 11 October 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-28 and 30 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-28 and 30 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>11/29/07</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This is in response to the RCE filed on 10/11/2007.
2. Claims 1-28 and 30 are pending in the application.
3. Claims 1-28 and 30 have been rejected.

Continued Examination Under 37 CFR 1.114

4. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10/11/2007 has been entered.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1-9, 19-27 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. In these claims applicants mention “**storing at least.....of a host processor.....generated by an input/output (“I/O”) processor....**”, “ **receiving....a host processor.....input/output (“I/O”)**”

processor....", which is generally narrative and indefinite with the invention.

Applicants do not point out clearly which options include in the present invention by these two controversial terms. Examiner confuses that the host processor and I/O processor which actually generates the encrypted data is the same processor or two different processors. This limitation made the whole claims ambiguous to understand for any ordinary skilled in the art. So, this limitation is indefinite with the present application. The examiner will interpret these terms and limitations with the regarding claim as best understood for applying the appropriate art for rejection purposes. Appropriate correction needs to overcome the rejection.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

The USPTO "Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility" (Official Gazette notice of 22 November 2005), Annex IV, reads as follows:

Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." In this context, "functional descriptive material" consists of data structures and computer programs which impart functionality when employed as a computer component. (The definition of "data structure" is "a physical or logical relationship among data elements, designed to support specific data manipulation functions." The New IEEE Standard Dictionary of Electrical and Electronics Terms 308 (5th ed. 1993).) "Nonfunctional descriptive material" includes but is not limited to music, literary works and a compilation or mere arrangement of data.

When functional descriptive material is recorded on some computer-readable medium it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized. Compare *In re Lowry*, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994) (claim to data structure stored on a computer readable medium that increases computer efficiency held statutory) and *Warmerdam*, 33 F.3d at 1360-61, 31 USPQ2d at 1759 (claim to computer having a specific data structure stored in memory held statutory product-by-process claim) with *Warmerdam*, 33 F.3d at 1361, 31 USPQ2d at 1760 (claim to a data structure per se held nonstatutory).

In contrast, a claimed computer-readable medium encoded with a computer program is a computer element which defines structural and functional interrelationships between the computer program and the rest of the computer which

permit the computer program's functionality to be realized, and is thus statutory. See Lowry, 32 F.3d at 1583-84, 32 USPQ2d at 1035.

6. Claims 19-27 are rejected under 35 U.S.C. 101 because the claim invention is directed to non-statutory subject matter. According to the specification of the invention (Page 1-25) "**An Article**" is reasonably interpreted by one of ordinary skill as just software, it is a system of software, per se. In this claim the function of the article is just software not any hardware. No where in the specification of this application mention what does the article means. All the dependent claims indicate that an article is just software, not any tangible hardware. Compare Warmerdam, 33 F.3d at 1361, 31 USPQ2d at 1760 (claim to a data structure per se held nonstatutory). Such claimed data structures do not define any structural and functional interrelationships between the data structure and other claimed aspects of the invention which permit the data structure's functionality to be realized. Similarly, computer programs claimed as computer instructions per se, i.e., the descriptions or expressions of the programs, are not physical "things." They are neither computer components nor statutory processes, as they are not "acts" being performed. Such claimed computer programs do not define any structural and functional interrelationships between the computer program and other claimed elements of a computer which permit the computer program's functionality to be realized. Accordingly, it is important to distinguish claims that define descriptive material per se from claims that define statutory inventions. So, it does not appear that a claim reciting software with functional descriptive material falls within any of the categories of patentable subject matter set forth in § 101.

Response to Arguments

7. Applicant's arguments with respect to claims 1-28 and 30 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-28 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kashima et al hereinafter Kashima (U.S. Patent No. 5485598) in view of Murthy et al hereafter Murthy (US patent publication 20030084290).

9. As per claims 1, Kashima discloses a method comprising: generating, based upon the one or more respective portions of the encrypted write data, check data to be stored in the storage (col. 3, lines 30-53); and selecting the one or more locations so as to permit the one or more respective portions of the encrypted write data to be

distributed among two or more storage devices comprised in the storage (col. 2, lines 5-12, claims 1-19). He does not expressly disclose storing at least one key within a tamper detection boundary of a circuit card coupled to a system bus of a host processor; encrypting, based upon the at least one key, one or more respective portions of write data to generate one or more respective portions of encrypted write data to be stored in one or more locations in a storage coupled to the system bus, the write data generated by an input/output ("I/O") processor on the circuit card. However, in the same field of endeavor, Murthy discloses encrypting, based upon the at least one key, one or more respective portions of write data to generate one or more respective portions of encrypted write data to be stored in one or more locations in a storage coupled to the system bus (paragraph, 0010-0012, 0016), storing at least one key within a tamper detection boundary of a circuit card coupled to a system bus of a host processor; the write data generated by an input/output ("I/O") processor on the circuit card (paragraph, 0030, 0033-0034).

Accordingly, it would been obvious to one of ordinary skill in the network security art at the time of invention was made to have incorporated Murthy's teachings of generating the encrypted write data from a secure host processor with the teachings of Kashima, for the purpose of suitably using the encrypted write data produced by secure host processor to store in plurality of storage devices (paragraph, 0010-0012, 0016).

10. As per claims 2, Kashima discloses the method wherein: the storage comprises a redundant array of independent disks (RAID); and the check data comprises one of parity data and a copy of the encrypted write (col. 3, lines 30-53).

11. As per claims 3, Kashima does not disclose the method wherein: in response-to an attempt to tamper with the at least one key, erasing the at least one key. However, Murthy discloses wherein: in response-to an attempt to tamper with the at least one key, erasing the at least one key (paragraph, 0030, 0033-0034).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 3.

12. As per claims 4, Kashima discloses the method comprising: determining, based upon one or more credentials, whether to permit execution of one or more operations involving the storage (col. 3, lines 30-53).

13. As per claims 5, Kashima discloses a method comprising: one or more respective portions of the encrypted read data retrieved from the storage to generate one or more respective portions of read data (col. 2, lines 5-12, claims 1-19). He does not expressly disclose receiving a read request from a host processor; retrieving one or more respective portions of [[the]] encrypted data from a plurality of storage devices comprised in [[the]] a storage coupled to the host processor; and decrypting, based upon at least one key stored within a tamper detection boundary of an encryption device coupled to the host processor, the read data generated by an input/output (I/O) processor located within the tamper detection boundary of the encryption device. However, Murthy discloses receiving a read request from a host processor; retrieving one or more respective portions of [[the]] encrypted data from a plurality of storage devices comprised in [[the]] a storage coupled to the host processor (paragraph, 0010-

0012, 0016); and decrypting, based upon at least one key stored within a tamper detection boundary of an encryption device coupled to the host processor, the read data generated by an input/output (I/O) processor located within the tamper detection boundary of the encryption device (paragraph, 0030, 0033-0034).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 5.

14. As per claims 6, Kashima discloses the method comprising: prior to the decrypting of the one or more respective portions of the encrypted data, determining, based upon one or more credentials, whether the request is authorized (col. 2, lines 5-12, claims 1-19).

15. As per claims 7-9, Kashima discloses the method generating the at least one key based upon at least one of one or more tokens and one or more passwords, the storage also stores metadata; and the method further comprises encrypting the metadata based upon the at least one key, wherein the metadata comprises partition information (col. 2, lines 5-12, claims 1-19).

16. As per claims 10, Kashima discloses an apparatus comprising: the circuitry also being capable of: generating, based upon the one or more respective portions of the encrypted write data, check data to be stored in the storage; and selecting the one or more locations so as to permit the one or more respective portions of the encrypted write data to be distributed among two or more storage devices comprised in the storage (col. 2, lines 5-12, claims 1-19). He does not expressly disclose circuitry to

encrypt, based upon at least one key stored within a tamper detection boundary, one or more respective portions of write data to generate one or more respective portions of encrypted write data to be stored in one or more locations in storage. However, Murthy discloses one or more respective portions of write data to generate one or more respective portions of encrypted write data to be stored in one or more locations in storage (paragraph, 0010-0012, 0016) circuitry to encrypt, based upon at least one key stored within a tamper detection boundary (paragraph, 0030, 0033-0034).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 10.

17. As per claims 11, Kashima discloses the apparatus wherein: the storage comprises a redundant array of independent disks (RAID); and the check data comprises one of parity data and a copy of the encrypted write data (col. 2, lines 5-12, claims 1-19).

18. As per claims 12, Kashima discloses the apparatus wherein: the circuitry is also capable of storing the at least one key in memory (col. 2, lines 5-12, claims 1-19). He does not expressly disclose in response to an attempt to tamper with the at least one key, erasing the at least one key from the memory. However, Murthy discloses in response to an attempt to tamper with the at least one key, erasing the at least one key from the memory (paragraph, 0030, 0033-0034).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 12.

19. As per claims 13, and 14 Kashima discloses the apparatus wherein: the circuitry is also capable of determining, based upon one or more credentials, whether to permit execution of one or more operations involving the storage (col. 3, lines 30-53 circuit to receive a read request, retrieve one or more respective portions of the encrypted data from [[a]] the plurality of storage devices comprised in the storage and decrypting, based upon at least one key, one or more respective portions of the encrypted read data retrieved from the storage to generate one or more respective portions of read data (col. 2, lines 5-12, claims 1-19).

20. As per claims 15-16, Kashima discloses the apparatus wherein the circuitry is also capable of: prior to the decrypting of the one or more respective portions of the encrypted data, determining, based upon one or more credentials, whether the request is authorized, and wherein: the circuitry is also capable of generating the at least one key based upon at least one of one or more tokens and one or more passwords (col. 2, lines 5-12, claims 1-19).

21. As per claims 17-18, Kashima discloses the apparatus wherein: the storage also stores metadata; and the circuitry is also capable of encrypting the metadata based upon the at least one key, the metadata comprises partition information (col. 2, lines 5-12, claims 1-19).

22. As per claims 19, Kashima discloses an article comprising: generating, based upon the one or more respective portions of the encrypted write data, check data to be stored in. the storage (col. 3, lines 30-53); and selecting the one or more locations so as

to permit the one or more respective portions of the encrypted write data to be distributed among two or more storage devices comprised in the storage (col. 2, lines 5-12, claims 1-19). He does not expressly disclose encrypting, based upon the at least one key, one or more respective portions of write data to generate one or more respective portions of encrypted write data to be stored in one or more locations in a storage coupled to the system bus (paragraph, 0010-0012, 0016), storing at least one key within a tamper detection boundary of a circuit card coupled to a system bus of a host processor; the encrypted write data generated by an input/output processor on the circuit card. However, Murthy discloses (paragraph, 0030, 0033-0034).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 19.

23. As per claims 20, and 22 Kashima discloses the article wherein: the storage comprises a redundant array of independent disks (RAID); and tile check data comprises one of parity data and a copy of the encrypted write data, wherein, the instructions when executed by the machine also result in: determining, based upon one or more credentials, whether permit execution of one or more operations involving the storage (col. 2, lines 5-12, claims 1-19).

24. As per claims 21 Kashima does not disclose the article wherein the instructions when executed by the machine also result in: storing the at least one key in memory; and in response to an attempt to tamper with the at least one key, erasing the at least one key. However, Murthy discloses storing the at least one key in memory; and in

response to an attempt to tamper with the at least one key, erasing the at least one key (paragraph, 0030, 0033-0034).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 21.

25. As per claims 23 Kashima discloses an article comprising receiving a read request from a host processor; one or more respective portions of the encrypted read data retrieved from the storage to generate one or more respective portions of read data (col. 2, lines 5-12, claims 1-19). He does not expressly disclose retrieving one or more respective portions of [[the]] encrypted data from a plurality of storage devices comprised in [[the]] a storage coupled to the host processor; and decrypting, based upon at least, one key stored within a tamper detection boundary of an encryption device coupled to the host processor, the read data generated by an input/output processor located within the tamper detection boundary of the encryption device. However, Murthy discloses retrieving one or more respective portions of [[the]] encrypted data from a plurality of storage devices comprised in [[the]] a storage coupled to the host processor (paragraph, 0010-0012, 0016); and decrypting, based upon at least, one key stored within a tamper detection boundary of an encryption device coupled to the host processor, the read data generated by an input/output processor located within the tamper detection boundary of the encryption device (paragraph, 0030, 0033-0034).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 23.

26. As per claims 24, and 25 Kashima discloses the article prior to the decrypting of the one or more respective portions of the encrypted data, determining, based upon one or more credentials, whether the request is authorized, wherein the instructions when executed by the machine also result in: generating the at least one key based upon at least one of one or more tokens and one or more passwords (col. 2, lines 5-12, claims 1-19).

27. As per claims 26, and 27 Kashima discloses the article wherein: the storage also stores metadata; and the instructions when executed by the machine also result in. encrypting the metadata based upon the at least one key, the metadata comprises partition information (col. 2, lines 5-12, claims 1-19).

28. As per claims 28 Kashima discloses a system comprising: generating, based upon the one or more respective portions of the encrypted write data, check data to be stored in the storage; and selecting the one or more locations so as to permit the one or more respective portions of the encrypted write data to be distributed among two or more storage devices comprised in the storage (col. 2, lines 5-12, claims 1-19). He does not expressly disclose a circuit board comprising a circuit card slot and a circuit card that is capable of being inserted into the circuit card slot, the circuit card comprising circuitry, the circuitry being capable of encrypting, based upon at least one key, one or

more respective portions of write data to generate one or more respective portions of encrypted write data to be stored in one or more locations in storage [[:]], wherein the circuitry also is capable of: wherein the circuit comprises: an input/output (i/O) processor, and non-volatile memory that is capable of storing the at least one key wherein the circuitry is capable of detecting-an attempt to tamper with. The at least one key, and in response to the attempt, erasing the at least one key from the memory. However, Murthy discloses a circuit board comprising a circuit card slot and a circuit card that is capable of being inserted into the circuit card slot, the circuit card comprising circuitry, the circuitry being capable of encrypting, based upon at least one key, one or more respective portions of write data to generate one or more respective portions of encrypted write data to be stored in one or more locations in storage (paragraph, 0010-0012, 0016) [[:]], wherein the circuitry also is capable of: wherein the circuit comprises: an input/output (i/O) processor, and non-volatile memory that is capable of storing the at least one key wherein the circuitry is capable of detecting-an attempt to tamper with. The at least one key, and in response to the attempt, erasing the at least one key from the memory (paragraph, 0030, 0033-0034).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 28.

29. As per claims 30 Kashima discloses the system wherein[[:]] the circuit board also comprises a host processor coupled to the circuit card slot via a bus[[, and]]; one or more token memories to store one or more tokens; and additional circuitry to read one or more additional tokens stored in a removable

token memory after the removable token memory is inserted into a token reader (col. 2, lines 5-12, claims 1-19).


Conclusion

30. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mohammad w. Reza whose telephone number is 571-272-6590. The examiner can normally be reached on M-F (9:00-5:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, MOAZZAMI NASSER G can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


1/4/08

Mohammad Wasim Reza

AU 2136